RANCANG BANGUN DAN PERBANDINGAN PERFORMA KERJA *PROTOCOL* VPN PPTP DAN L2TP/IPSec MEMANFAATKAN *IP PUBLIC DYNAMIC*

Deka Alfian Diazcha [(1)], Ali Khumaidi [(2)], Nurhikmah [(3)]
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Krisnadwipayana

E-mail: dekaalfiandiazcha@gmail.com [(1)], alikhumaidi@unkris.ac.id [(2)], nurhikmahiik4@gmail.com [(3)]

ABSTRACT

Virtual Private Network (VPN) is a computer network solution that uses public network infrastructure such as the internet by providing secure access to local networks. VPN by utilizing IP Public Dynamic offers savings in terms of operational costs that should be made with Public Static IP. Some MSMEs that run in the field of fashion (Distro), especially in Bekasi City use internet facilities to provide convenience in accessing MSME data such as item data master reports, stock reports, purchase reports, sales reports (per cashier user), cash drawer reports, reports accounts payable and income statement. Considering the importance of security and the speed of communication between networks in UMKM Distro, the VPN can be an alternative choice to provide a secure and fast network. VPN uses tunneling methods on public networks using protocols such as Point to Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol with IP Security (IPSec). Both protocols provide different levels of security, speed, and performance on a network which will then be analyzed so that it can become an alternative choice in providing access services in the UMKM Distro network.

Keywords : Virtual Private Network (VPN), Tunneling, Public Dynamic IP, PPTP, L2TP / IPSec

1. PENDAHULUAN

Dengan semakin berkembangnya teknologi informasi yang sangat pesat pada zaman sekarang ini. Munculnya teknologi-teknologi baru sangat membantu dalam kegiatan bisnis suatu usaha. Selain didukung teknologi terbaru, kebutuhan akan informasi secara *real time,* kinerja pada suatu jaringan merupakan suatu faktor penting dalam keberhasilan bisnis suatu usaha. Untuk mendukung keberhasilan tersebut, maka dibutuhkannya suatu teknologi yang dapat digunakan untuk menghubungkan perangkat yang berada diluar jaringan *Intranet*. Teknologi tersebut harus aman digunakan dalam pertukaran data, aman dari kemungkinan aksi *hacking* dan data *sniffing* di dalam *internet* yang dapat di akses oleh orang-orang di dunia. Maka dari itu dibuat jaringan *virtual* yang hanya bisa digunakan oleh orang-orang yang mempunyai wewenang untuk mengakses data tersebut, yaitu jaringan pribadi atau disebut juga *Virtual Private Network* (VPN) (Wibowo, Abimanyu. 2012).

Pemanfaatan VPN di dalam menjalankan bisnis suatu usaha sangat diperlukan khususnya bagi Usaha Micro Kecil Menengah (UMKM). Tetapi dari beberapa hasil penelitian sebelumnya tingkat dari para pelaku UMKM untuk mengandalkan teknologi informasi masih sangat kurang, karena mereka memiliki beberapa faktor diantaranya dari segi SDM dan *financial*. Penelitian yang dilakukan pada UMKM di bidang fashion (Distro) khususnya di daerah Kota Bekasi, mereka sudah dapat menerapkan teknologi informasi pada usahanya. Namun, kekurangan dari UMKM distro tersebut ialah mengenai keamanan dalam mensharing data, dimana penggunaan *email* yang mereka lakukan dalam melakukan *sharing* data memberikan celah bagi para *hacker* untuk dapat menyerang lalu lintas pengiriman data yang dilakukan UMKM distro. Kesempatan inilah yang nantinya dimanfaatkan para *hacker* untuk dapat mencuri data penting pada UMKM distro. Dari penelitian yang dilakukan pada UMKM distro di kota bekasi, kasus mengenai hilangnya data dan kesalahan data pada saat *sharing* data menggunakan *email* sangat banyak. Sehingga perlu adanya sistem baru untuk dapat menjaga keamanan di dalam jalur *sharing* data yang dilakukan pada UMKM distro. Karena kebutuhan akan data secara cepat pada UMKM distro sangat diperlukan, sehingga membuat UMKM distro menggunakan *email* sebagai alat dalam mensharing data yang mereka anggap mempermudah dalam mensharing data. Adapun cara lainnya dengan mereka memprint out data UMKM distro tersebut untuk dapat di *sharing*. Dalam hal ini keamanan data dalam transmisi sebuah jaringan komputer merupakan faktor yang sangat penting. Maka dari itu dibutuhkan sebuah teknologi informasi keamanan untuk dapat menjaga jalur akses dalam mensharing data penting pada UMKM distro. Teknologi informasi tersebut berupa VPN.

Karena dengan adanya VPN, UMKM distro dapat mensharing data dengan sangat

efisien, dan memberikan keamanan serta fleksibelitas terhadap data-data yang di *sharing*. Dalam hal ini, VPN sangat dibutuhkan untuk dapat menjembatani akses dalam mensharing data yang dilakukan UMKM distro secara aman tanpa adanya gangguan dari pihak luar. Nantinya VPN ini dibentuk memanfaatkan *IP Public Dynamic*, dimana UMKM distro tidak usah mengeluarkan anggaran untuk menyewa *IP Public Static* dalam pembentukkan jalur VPN ini. Adapun *protocol* yang nantinya akan digunakan yaitu PPTP dan L2TP/IPSec, keduanya dirasa cukup dijadikan *protocol* pada VPN untuk UMKM distro, dikarenakan kemudahannya dalam konfigurasi sehingga tidak terlalu menyulitkan SDM yang ada dalam mengelola ataupun membangun ulang jalur VPN tersebut nantinya. *Protocol* tersebut nantinya akan dibandingkan satu samalain guna mendapatkan hasil untuk dijadikan acuan *protocol* mana yang benar-benar cocok untuk UMKM distro. Parameter perbandingan yang dibandingkan disini ialah dari segi keamanan, kemudahan dalam konfigurasi, serta kecepatan dalam mengakses data yang dilakukan pengguna. Oleh sebab itu saya berkeinginan mengangkat judul "Rancang Bangun Dan Perbandingan Performa Kerja *Protocol* VPN PPTP Dan L2TP/IPSec Memanfaatkan IP *Public Dynamic*".

2. METODOLOGI PENELITIAN

A. Metode Pengumpulan Data Dalam mengumpulkan data untuk pengembangan sistem ini dilakukan dengan cara:

1. Observasi
2. Kuesioner
3. Penelitian Kepustakaan

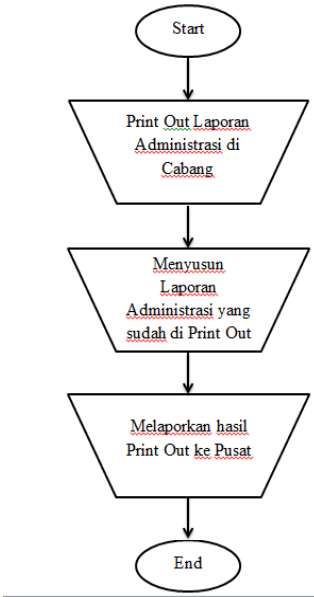
B. Metode pengembangan penelitian yang digunakan dalam penyusunan tugas akhir ini dengan menggunakan:

1. Studi Literatur
   Studi literatur dilakukan dengan mengumpulkan data-data atau sumber-sumber yang berhubungan dengan topik penelitian ini untuk digunakan sebagai refrensi selama penelitian.
2. Analisis
   Pada tahap ini dilakukan analisis terhadap jaringan VPN menggunakan *IP Public Dynamic*, baik dari segi kegunaannya bagi UMKM distro, serta analisis *protocol* yang akan digunakan VPN.
3. Implementasi
   Pada tahap ini dilakukan implementasi terhadap VPN menggunakan *IP Public Dynamic*, dimulai dari konfigurasi VPN sampai hasil setelah konfigurasi VPN selesai dibentuk.
4. Pengujian
   Dari semua tahap dalam proses membangun VPN, akan dilakukan pengujian untuk mendapatkan kesimpulan dari hasil pengujian VPN yang telah di implementasikan.

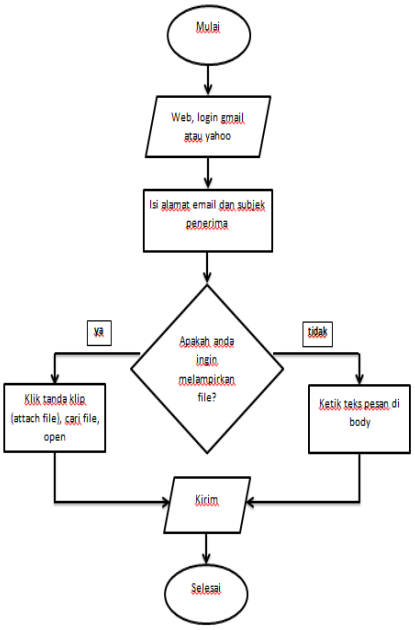
3. ANALISA DAN PERANCANGAN

a. Analisa Sistem Jaringan Berjalan

Berdasarkan penelitian yang telah dilakukan pada pelaku UMKM, aktifitas dalam mensharing data penting UMKM ke kantor pusat masih dilakukan dengan cara konvensional dan menggunakan aplikasi berbasis website.



Gambar 1. *Flowchart* Aktifitas *Sharing* Data Konvensional

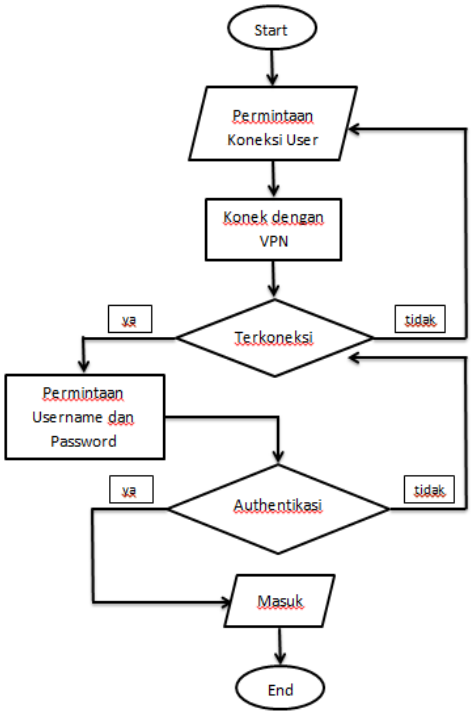


Gambar 2. *Flowchart* Aktifitas *Sharing* Data Menggunakan E-mail

b. Sistem Jaringan yang diusulkan

Mensharing data penting UMKM yang dilakukan dengan cara konvensional dan menggunakan aplikasi berbasis website saat ini memakan banyak waktu dan juga kurang aman dari aksi *hacking* dan *sniffing* pihak luar, maka dengan permasalahan yang ada dibutuhkan suatu jaringan yang lebih efisien di dalam penggunaannya maupun keamanannya. Sistem jaringan yang diusulkan berupa jalur Virtual Private Network (VPN) dimana teknologi ini memiliki efisiensi dan keamanan dari aksi *hacking* dan *sniffing* pihak luar. Sistem jaringan ini di khususkan bagi para perusahaan yang ingin mencoba memanajemen keamanan datanya sendiri sehingga meminimalisir para *hacking* maupun pihak luar untuk dapat masuk ke sistem jaringan yang di khususkan ini.

Pada tahap pembentukkan jaringan ini nantinya akan digunakan *IP Public Dynamic*, yang mana fungsinya sebagai jalur VPN yang akan dibentuk dan juga dengan adanya *IP Public Dynamic* meminimalisir dana yang diperlukan untuk membangun teknologi jaringan VPN.



Gambar 3. Flowchart Sistem VPN yang diusulkan pada UMKM (Distro)

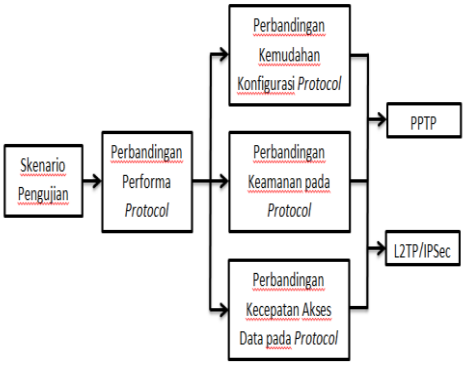
c. Skenario Pengujian

Setelah merancang topologi yang akan digunakan dalam pembentukkan VPN untuk penggunaan *protocol* PPTP dan L2TP/IPSec, tahap selanjutnya adalah scenario pengujian yang akan dilakukan dengan tahap-tahap Perbandingan Hasil Pengujian.

Tahapan selanjutnya setelah implementasi adalah melakukan uji coba dan testing. Testing dilakukan terhadap koneksi VPN yang telah dibuat. Pengujian koneksi ini dapat dilakukan berulang kali untuk mendapatkan hasil implementasi VPN yang stabil. Pengujian koneksi VPN ini dilakukan untuk melihat apakah hasil implementasi sudah berjalan sesuai dengan yang diharapkan. Jika masih bermasalah, maka evaluasi tehadap penelitian ini harus dilakukan.

Pada tahap ini, pengambilan data akan dilakukan setelah proses implementasi selesai pada konfigurasi, serta setelah proses *sniffing* menggunakan perangkat lunak *wireshark*. Dan pengambilan data kecepatan dalam mengakses data pada *protocol* PPTP dan L2TP/IPSec dilakukan dengan cara mendownload data berformat pdf, mp3, dan mp4.

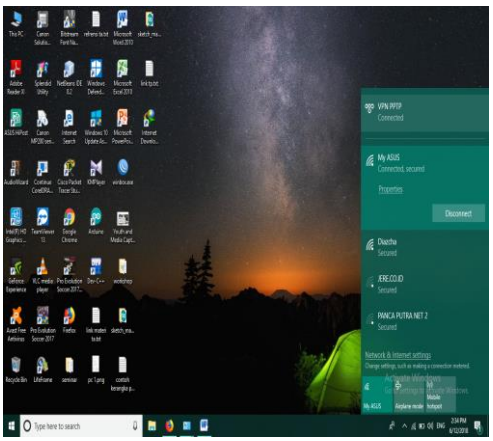
Data untuk perbandingan keamanan kedua *protocol tunneling* nantinya diambil dari banyaknya fitur keamanan yang dikonfigurasi serta bukti terbentuknya keamanan pada masing-masing *protocol*.



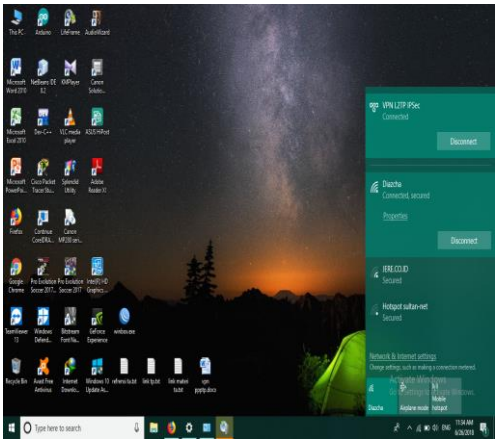
Gambar 4. Skenario Pengujian Perbandingan *Protocol*

4. HASIL DAN PEMBAHASAN

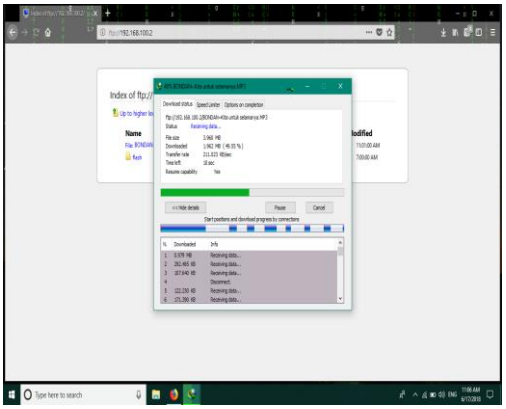
a. Pengujian Sistem Jaringan



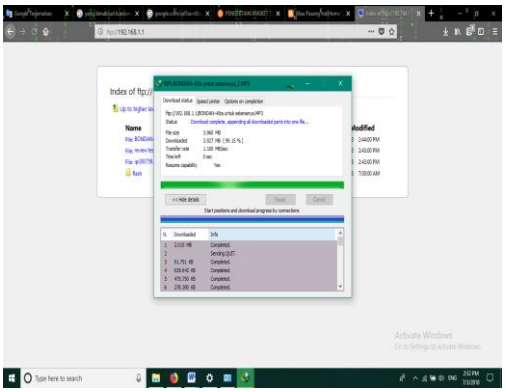
Gambar 5. *Connected* VPN PPTP



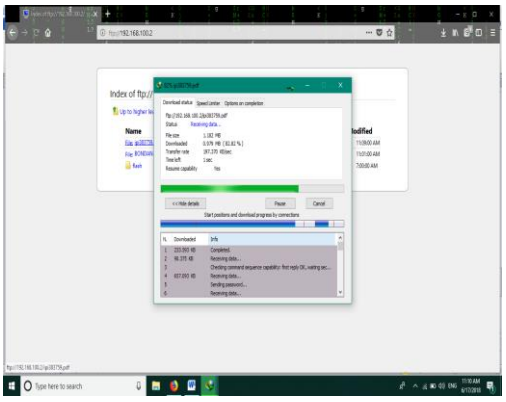
Gambar 6. Connected VPN L2TP/IPSec



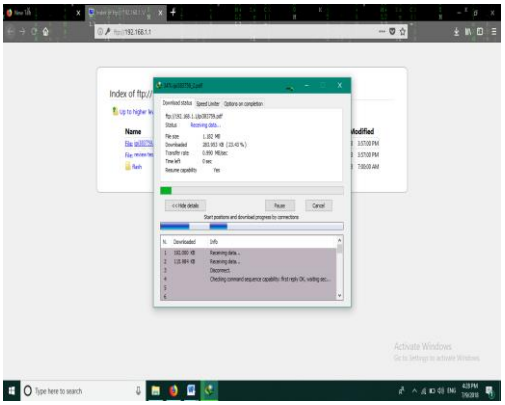
Gambar 7. *Download* Format MP3 *Protocol* VPN PPTP



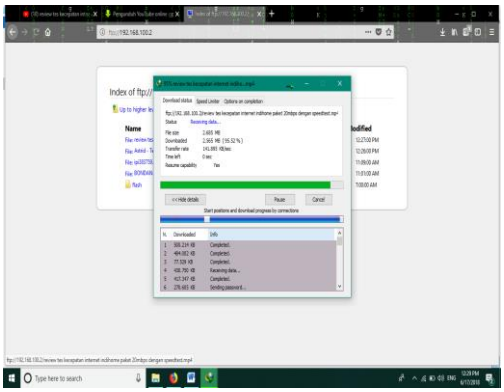
Gambar 8. *Download* Format MP3 *Protocol* VPN L2TP/IPSec



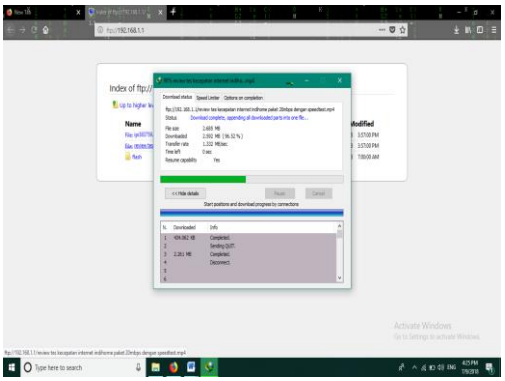
Gambar 9. *Download* Format PDF *Protocol* VPN PPTP



Gambar 10. *Download* Format PDF *Protocol* VPN L2TP/IPSec

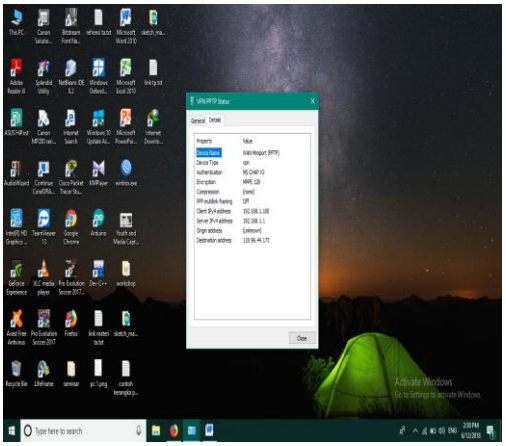


Gambar 11. *Download* Format MP4 *Protocol* VPN PPTP



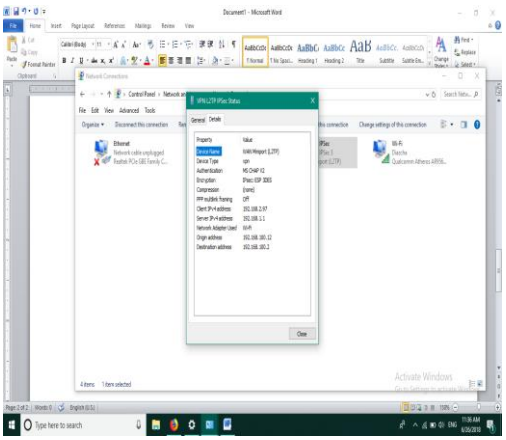
Gambar 12. *Download* Format MP4 *Protocol* VPN L2TP/IPSec

Pada VPN PPTP *Authentication* yang digunakan yaitu MS CHAP V2, metode ini untuk memvalidasi user yang ingin terkoneksi dengan megidentifikasi *hostname client*. Sedangkan untuk *Encryption* yang digunakan pada *protocol* VPN PPTP yaitu MPPE 128, *Microsoft Point-to-Point Encryption* (MPPE) mengenkripsi data dalam koneksi *dial-up Point-to-Point Protocol* (PPP) atau koneksi *Protokol* Penerobosan Titik-ke-Titik (PPTP) VPN.



Gambar 13. Status *Authentication* dan *Encryption Protocol* VPN PPTP

Untuk *Authentication* yang digunakan pada *protocol* VPN L2TP/IPSec yaitu MS CHAP V2, metode ini untuk memvalidasi user yang ingin terkoneksi dengan mengindetifikasi *hostname client*. Sedangkan untuk *Encryption* yang digunakan pada *protocol* VPN L2TP/IPSec yaitu IPSec: ESP dan 3DES



Gambar 14. Status *Authentication* dan *Encryption Protocol* VPN L2TP/IPSec

b. Perbandingan Sebelum Menggunakan VPN dan Sesudah Menggunakan VPN *Protocol* PPTP dan *Protocol* L2TP/IPSec

Tabel 1. Perbandingan *Protocol* VPN

Parameter Perbandingan	Sebelum Menggunakan VPN	Sesudah Menggunakan VPN	
		Protocol VPN	Protocol VPN L2TP/IPS

		PPTP	**ec**
Keamanan	Keamanan pada saat sebelum dilakukannya konfigurasi *protocol* VPN masih sangat kurang baik, karena tidak adanya jaminan keamanan pada akses data yang dimiliki UMKM distro, seperti halnya keamanan yang ditawarkan *protocol* VPN PPTP dan L2TP/IPSec yang berupa Authentication maupun Encryption.	Keamanan yang digunakan *protocol* VPN PPTP ini yaitu dari segi authentication dan encryption, yang mana Authentication yang digunakan yaitu MS CHAP V2 dan Encryption yang digunakan yaitu *Microsoft Point-to-Point Encryption* (MPPE).	Keamanan yang digunakan *protocol* VPN L2TP/IPSec ini yaitu dari segi authentication dan encryption, yang mana Authentication yang digunakan sama dengan *protocol* VPN PPTP yaitu MS CHAP V2 dan Encryption yang digunakan yaitu IPSec: ESP dan 3DES.
Kemudahan Dalam Konfigurasi	Karena sharing data dilakukan via email sehingga tidak ada konfigurasi yang harus dibuat dalam membentuk jalur keamanan.	Dilihat dari hasil implementasi yang dilakukan, pembentukkan *protocol* VPN PPTP ini sangat mudah untuk dapat di konfigurasi. Sehingga memudahkan user dalam membentuk sebuah jalur VPN menggunakan *protocol* ini.	Dilihat dari hasil implementasi yang dilakukan, pembentukkan *protocol* VPN L2TP/IPSec ini lebih sulit dibanding *protocol* VPN PPTP untuk dapat di konfigurasi. Tetapi masih bisa untuk dipahami user untuk dapat dibentuk sebuah jalur VPN menggunakan *protocol* ini.
Kecepatan Dalam Mengakses Data	Kecepatan dalam mengakses data yang dimiliki sebelum terbentuknya jalur VPN sangat baik, karena tidak adanya keamanan yang dibentuk dari jalur akses data tersebut.	Setelah dilakukannya testing pada *protocol* VPN PPTP ini, di dapatkan hasil bahwa kecepatan *protocol* VPN ini lebih cepat dibandingkan *protocol* VPN L2TP/IPSec.	Setelah dilakukannya testing pada *protocol* VPN L2TP/IPSec ini, di dapatkan hasil bahwa kecepatan *protocol* VPN ini lebih lambat dibandingkan *protocol* VPN PPTP dikarenakan keamanan tambahan yang diberikan IPSec.

5. KESIMPULAN

Setelah melakukan implementasi terhadap pembentukkan jalur VPN, dapat ditarik kesimpulan sebagai berikut :

1. Sebuah VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan *local* yang luas, karena transmisi data teknologi VPN menggunakan media jaringan *public* yang sudah ada.
2. Kemampuan teknologi informasi VPN ini membentuk jaringan LAN yang tidak di batasi tempat dan waktu, karena koneksitasnya dilakukan via *internet*.
3. Teknologi informasi VPN yang di implementasikan ini dapat mempermudah pengguna dalam melakukan pertukaran data dan informasi yang aman dari tempat yang berbeda dan berjauhan.
4. Penggunaan *IP Public Dynamic* dapat menekan anggaran pembentukkan VPN menggunakan *IP Public Static*. Penggunaan *IP Public Dynamic* juga memberikan manfaat, yaitu memanfaatkan *IP Public Dynamic* yang disediakan ISP tanpa menyewa *IP Public Static*.
5. Hasil dari perbandingan *protocol* yang digunakan, menghasilkan sebuah perbandingan sebagai berikut :
   - *Protocol* PPTP memiliki kemudahan yang lebih dalam mengkonfigurasi pembentukan jalur VPN serta memiliki kecepatan dalam megakses data.

Tetapi dari segi keamanan, keamanan *protocol* L2TP/IPSec yang lebih baik dibandingkan *protocol* PPTP.

- *Protocol* L2TP/IPSec memiliki keamanan yang lebih, sebab *protocol* L2TP di bentuk bersamaan dengan IPSec yang merupakan keamanan tambahan pada pembentukkan jalur VPN. Tetapi dilihat dari segi kemudahan dalam konfigurasi dan kecepatan akses data, *protocol* L2TP/IPSec memiliki tingkat kesulitan konfigurasi di atas *protocol* PPTP dan akses data yang dimiliki juga lebih lambat dibandingkan *protocol* PPTP.

6. DAFTAR PUSTAKA

1. Abdul Kadir. 2003. Pengenalan Sistem Informasi. ANDI Yogyakarta, Yogyakarta.
2. Agus Tedyyana dan Rezki Kurniati. (2016). Membuat Web *Server* Menggunakan *Dynamic Domain Name System* Pada IP Dinamis. BENGKALIS: PROGRAM STUDI POLITEKNIK NEGERI BENGKALIS.
3. Anjik Sukmaaji dan Rianto. 2008. "Jaringan Komputer : Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan", Andi Publisher. Yogyakarta.
4. Herlambang, M. L., dan Azis Catur L, 2008. Panduan Lengkap Menguasai Router Masa Depan Menggunakan MikroTik RouterOS, ANDI Publisher, Yogyakarta.
5. Indrajani, S. M. (2011). Modul Pembelajaran Rekayasa Perangkat Lunak. Bandung: Modula
6. Iwan, Sofana. 2012. Cisci CCNP & Jaringan Komputer. Bandung: Informatika
7. Krismiaji. 2010. Sistem Informasi Akuntansi. Edisi ketiga. Yogyakarta: Unit Penerbitan Dan Percetakan Sekolah Tinggi Manajemen YKPN.
8. Kristanto, Andri. 2003. Keamanan Data Pada Jaringan Komputer. Yogyakarta: Gava Media.
9. Martin, E.Wainright. et.al. 1999. Managing Information Technology What Managers Need to Know. Pearson Educational International. New Jersey.
10. Mikrotik Indonesia. (2013). Konfigurasi VPN PPTP pada Mikrotik. Retrieved from MIKROTIK INDONESIA: http://mikrotik.co.id/artikel_lihat.php?id=43. (Diakses 08 Mei 2018).
11. Pahlevy, 2010. Pengertian Flowchart dan definisi data.
12. (http://www.landasanteori.com /2015/10/pengertian-flowchart-dan definisi-data.html) diakses 8 Mei 2018.
13. Ramdhani, A. Y. (2010). PERACANGAN DAN IMPLEMENTASI VPN MENGGUNAKAN PROTOKOL PPTP DAN L2TP BERBASIS MIKROTIK, 2-7.
14. Siallagan, Sariadin. 2009. Pemrograman Java. Yogyakarta: Andi Yogyakarta.
15. Sofana, Iwan. 2012.
16. Sofana, Iwan. 2013. Membangun Jaringan Komputer : Mudah membuat Jaringan Komputer (Wire & Wireless) untuk pengguna Windows dan Linux. Bandung: Informatika.
17. Stephen Haag dan Peter G. W. Keen. 1996. Information Technology. McGraw-Hill.
18. Tanaenbaum, A. S. (2003). *Computer Networks*. New Jersey: Pearson Education.
19. Tanaenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks*.
20. Tona Aurora Lubis dan Junaidi. (2015). Pemanfaatan Teknologi Informasi pada Usaha Mikro Kecil dan Menengah di Kota Jambi. KOTA JAMBI: UNIVERSITAS JAMBI.
21. Triyono, J., Rachmawati, Y., & Irawan, F. D. (2014). ANALISIS PERBANDINGAN KINERJA JARINGAN VPN BERBASIS MIKROTIK MENGGUNAKAN PROTOKOL PPTP DAN L2TP SEBAGAI MEDIA TRANSFER DATA. Jurnal JARKOM, 112-120.
22. Wibowo, Abimanyu. (2012). PERBANDINGAN *TUNNELING PROTOCOL* PPTP dengan L2TP PADA JARINGAN VPN (*VIRTUAL PRIVATE NETWORK*) MENGGUNAKAN MIKROTIK RB750. JAKARTA: UNIVERSITAS ESA UNGGUL.
23. William, B.K., Sawyer, S.C. 2003. Using Information Technology A Practical Introduction to Computers & Communications. McGraw-Hill.
24. Yudianto, M. Jafar Noor. 2007. Diakses tanggal 8 Mei 2018, dari website Ilmu Komputer http://www.unej.ac.id/files/pdf2/Ilmu-komputer-Jaringan-Komputer-Dan-Pengertiannya.pdf

25. Yulyus Effendi Pradana, Jusak, dan Yosefine Triwidyastuti. (2016). Analisis Unjuk Kerja *Virtual Private Network* PPTP dan L2TP Pada Jaringan Berbasis *MikroTik*. SURABAYA: STIKOM SURABAYA.